(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 014 318 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
20.09.2000 Bulletin 2000/38

(43) Date of publication A2:
28.06.2000 Bulletin 2000/26

(21) Application number: **99125264.4**

(22) Date of filing: **17.12.1999**

(51) Int. Cl.[7]: **G07F 17/42**, G07B 1/02

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **18.12.1998 JP 36072098**

(71) Applicant:
KABUSHIKI KAISHA TOSHIBA
Kawasaki-shi, Kanagawa-ken 210-8520 (JP)

(72) Inventor:
Yamaguchi, Takashi,
Int. Property Division
Tokyo 105-8001 (JP)

(74) Representative:
Blumbach, Kramer & Partner GbR
Radeckestrasse 43
81245 München (DE)

(54) Ticket issuing method, ticket issuing system and ticket collating method

(57) In a ticket issuing method, security data is first made from ticket issue request data and user identification data sent from user via a communication means and then, ticket image data is made from the ticket issue request data and by embedding the security data in the ticket image data in the invisible state, ticket printing data for printing ticket by user is made. The ticket printing data thus made is sent to user via a communication means.

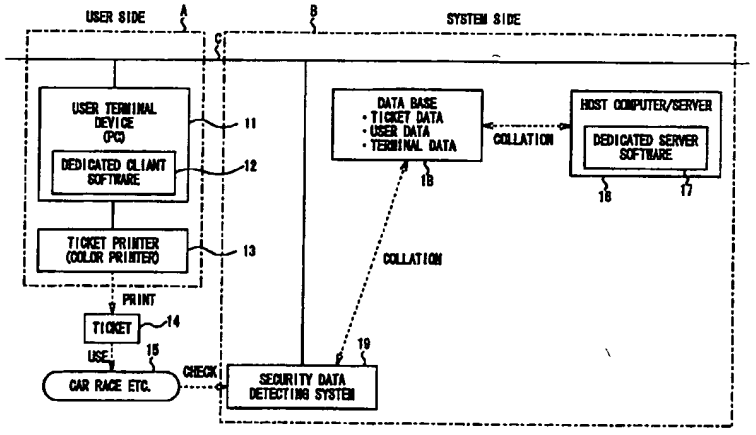

FIG. 1

EP 1 014 318 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 12 5264

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	US 5 598 477 A (BERSON WILLIAM) 28 January 1997 (1997-01-28)	1,15	G07F17/42 G07B1/02
A	* claim 1; figures 1,2 *	10,11,16	G07D7/12
Y	EP 0 581 317 A (INTERACTIVE HOME SYSTEMS) 2 February 1994 (1994-02-02)	1,15	
A	* page 2, line 26 - line 30 *	2,8	
A	US 5 731 880 A (KANNO AKIKO ET AL) 24 March 1998 (1998-03-24) * claim 1 *	3,11	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

G07D
G07F
G07B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	2 August 2000	Paraf, E

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 12 5264

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	US 5 598 477 A (BERSON WILLIAM) 28 January 1997 (1997-01-28)	1,15	G07F17/42 G07B1/02
A	* claim 1; figures 1,2 *	10,11,16	G07D7/12
Y	EP 0 581 317 A (INTERACTIVE HOME SYSTEMS) 2 February 1994 (1994-02-02)	1,15	
A	* page 2, line 26 - line 30 *	2,8	
A	US 5 731 880 A (KANNO AKIKO ET AL) 24 March 1998 (1998-03-24) * claim 1 *	3,11	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

G07D
G07F
G07B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	2 August 2000	Paraf, E

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Ticket issuing method, ticket issuing system and ticket collating method

Patent number: EP1014318
Publication date: 2000-06-28

Inventor: YAMAGUCHI TAKASHI (JP)
Applicant: TOKYO SHIBAURA ELECTRIC CO (JP)

Classification:
- international: G07F17/42; G07B1/02
- european: G07B1/02
Application number: EP19990125264 19991217
Priority number(s): JP19980360720 19981218

Also published as:
EP1014318 (A2)
JP2000182086 (A)
EP1014318 (B1)
DE69917417T (T2)
DE69917417D (T2)

Cited documents:
US5598477
EP0581317
US5731880

Abstract of **EP1014318**

In a ticket issuing method, security data is first made from ticket issue request data and user identification data sent from user via a communication means and then, ticket image data is made from the ticket issue request data and by embedding the security data in the ticket image data in the invisible state, ticket printing data for printing ticket by user is made. The ticket printing data thus made is sent to user via a communication means.

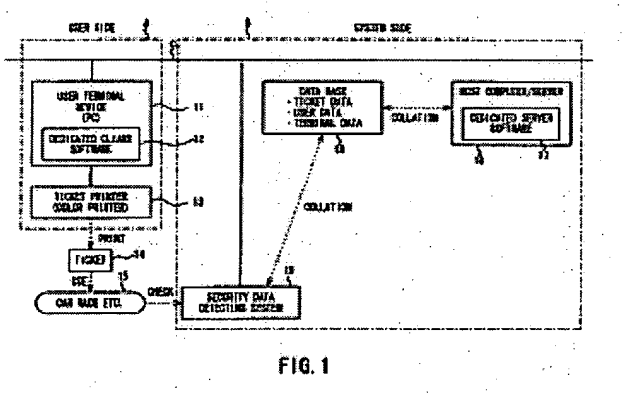

FIG. 1

Ticket issuing method, ticket issuing system and ticket collating method

Description of EP1014318

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The present invention relates to a ticket issuing method and a ticket issuing system to issue tickets, for instance, tickets for concerts, tickets of travelling facilities and other tickets by way of a network or a telephone line.

[0002] Further, the present invention relates to a ticket collating method for examining the genuineness of issued tickets.

2. Description of the Related Art

[0003] In recent years, a system is widespread to request tickets for concerts or transport facilities using a network or a telephone line and a requester goes to pick up the requested ticket at a prescribed place. Thus, it is possible to purchase tickets at home or a company.

[0004] Further, based on the widespread of personal computers and color printers and improvement of the infrastructure of the communication environment of the internet, etc., a system that is capable of directly issuing tickets that are requested via a network at home or a company is now under the examination.

[0005] Further, such a service is provided recently that when a ticket for a concert is requested via a network, an image for exchanging with a ticket is unloaded on a personal computer at home and record it on a floppy disk, that is then brought to the place of concert for listening the concert.

[0006] Further, a system is also being tested now to request an electronic postage stamp via a network and issue the requested electronic postage stamp at home or a company. For instance, U.S. Patent No. 5,696,507 and U.S. Patent No. 5,666,284, disclosed a method and a system to store postage stamp data including coded postal charge data in a dedicated storage device that is connected to a personal computer and print the stamp data on an envelope.

[0007] However, a dedicated storage device that is connected to a personal computer is required for the method and the system disclosed in U.S. Patent No. 5606,5007 and U.S. Paten No. 5,666,284 and therefore, a client system structure is restricted. Further, although a postal charge data is coded, it is printed in the visible state on an envelope using a two-dimensional code technology or its applied technology and therefore, there is such a defect that coded data is read relatively easily when a difference in two data is taken and compared and thus, its security is weak.

SUMMARY OF THE INVENTION

[0008] An object of the present invention is to provide a ticket issuing method and a ticket issuing system that are capable of simply issuing tickets that have high security by way of communication means such as a network or a telephone line.

[0009] In addition, another object of the present invention is to provide a ticket collating method that is capable of easily examining the genuineness of issued tickets and easily making a follow-up survey when any illegal ticket is detected.

[0010] According to the present invention, a ticket issuing method comprising the steps of making security data from ticket issue request data and user identification data sent from a user via a communication means; making ticket image data from the ticket issue request data; making ticket printing data by embedding the security data in the ticket image data, the security data being invisible against the ticket image data when the ticket printing data including the ticket image data and the security data is printed on a ticket paper by the user; and sending the ticket printing data to the user via a communication means, is provided.

[0011] Further, according to the present invention, a ticket collation method comprising the steps of: making security data from ticket issue request data and user identification data sent from a user via a communication means; making ticket image data from the ticket issue request data; making a prescribed pattern image data; making pattern modulated image data by modulating the prescribed pattern image data by the security data; making ticket printing data by superimposing the pattern modulated image data on the ticket image data; sending the ticket printing data to the user via a communication means; restoring the security data from a ticket printed by the user based on the received ticket printing data; and judging genuineness of the printed ticket according to the restored security data, is provided.

[0012] Further, according to the present invention, a ticket issuing system comprising: means for making security data from ticket issue request data and user identification data sent from a user via a communication means; means for making ticket image data from the ticket issue request data; means for making ticket printing data by embedding the security data in the ticket image data, the security data being invisible against the ticket image data when the ticket printing data including the ticket image data and the security data is printed on a ticket paper by the user; and means for sending the ticket printing data to the user via a communication means, is provided.

[0013] Further, according to the present invention, a ticket issuing method comprising the steps of: outputting security data according to ticket issue request data from a user via a communication means, the security data being visible when the security data is printed on a paper; outputting ticket image data from the ticket issue request data, the ticket image data being visible when the ticket image data is printed on a paper; outputting ticket printing data by embedding the security data in the ticket image data, the security data being invisible against the ticket image data when the ticket printing data including the ticket image data and the security data is printed on a ticket paper by the user; and sending the ticket printing data to the user via the communication means, is provided.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram schematically showing the structure of a ticket issuing system for achieving a ticket issuing method of the present invention;
FIG. 2 is a flowchart for explaining the operating steps of ticket issue;
FIG. 3 is a plan view showing an example of ticket image data when applied to an auto race admission ticket;
FIG. 4 is a plan view showing one example of security data when applied to an auto race admission ticket;

FIG. 5 is a plan view showing one example of ticket printing data when applied to an auto race admission ticket;
FIG. 6 is a schematic diagram for explaining the binary imaging of security data by two-dimensional code;
FIG. 7 is a schematic diagram for explaining the binary imaging of security data by two-dimensional code;
FIG. 8 is a schematic diagram for explaining the binary imaging of security data by two-dimensional code;
FIG. 9 is a block diagram for explaining the ticket printing data preparation step;
FIG. 10 is a diagram showing a definite calculation example in the ticket printing data making;
FIG. 11 is a diagram showing a definite calculation example in the ticket printing data making;
FIG. 12 is a diagram showing a definite calculation example in the ticket printing data making;
FIG. 13 is a diagram showing a definite calculation example in the ticket printing data making;
FIG. 14 is a diagram showing a definite calculation example in the ticket printing data making;
FIG. 15 is a diagram showing a definite calculation example in the ticket printing data making;
FIG. 16 is a diagram showing a definite calculation example in the ticket printing data making;

FIG. 17 is a diagram showing a definite calculation example in the ticket printing data making;
FIG. 18 is a diagram showing a definite calculation example in the ticket printing data making;
FIG. 19 is a diagram showing a definite calculation example in the ticket printing data making;
FIG. 20 is a diagram for explaining the thinning process in a third reproduction method;
FIG. 21 is a diagram for explaining an interpolation process in a third reproduction method;
FIG. 22 is a diagram schematically showing a ticket issuing method; and
FIG. 23 is a diagram for explaining an example when the ticket issue method of the present invention is applied to electronic postage stamps.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0015] Preferred embodiments of the present invention will be described below referring to the drawings.

[0016] FIG. 1 is a block diagram schematically showing the structure of a ticket issuing system to achieve the ticket issuing method of the present invention. This ticket issuing system is composed of by connecting a user side apparatus A with a system side apparatus B through such a network C as Internet, LAN, etc.

[0017] Further, "user" referred to here does mean a person who prints a ticket by a printer available at home and uses that ticket and a person who prints a ticket by a printer available at home or installed at a shop for use by other person or shop customer.

[0018] The user side apparatus A is composed of a user terminal device 11 comprising a personal computer, a dedicated client software 12 that operates on a personal computer, and a ticket printer 13 such as a color printer that is connected to the user terminal device 11.

[0019] The system side apparatus B is composed of a host computer/server 16, a dedicated server software 17 that operates on a host computer, a data base 18 that stores ticket data, user data and other data, and a security data detecting system 19.

[0020] Next, a ticket issue operating steps will be explained referring to a flowchart shown in FIG. 2. The host computer/server 16, the dedicated server software 17 and the data base 18 are always in the ready to operate state and users who are registered in the data base 18 are able to use anytime.

[0021] First, a user starts up the user terminal device 11 and the dedicated client software 12 (Step S1) and connects the user terminal device 11 to the host computer/server 16 (Step S5) by inputting user identification data such as a usr ID and a password (Step S2).

[0022] The host computer/server 16 collates the input user identification data with data stored in the data base 18 (Step S3) and approves the connection (Step S4) and starts the service when the input data is contained in the registered user list, and rejects the connection if it is not contained in the registered user list.

[0023] When connected to the host computer/server 16 (Step S5), a service menu is displayed on the user terminal device 11 and a user selects a desired service and input ticket issue request data (Step S8). The ticket issue request data referred to here are, in the case of, for instance, a ticket purchasing service, such required data as a kind of desired ticket, date and time, charge, seat reservation, charge paying means, etc.

[0024] When the ticket issue request data are input, the user terminal device 11 transmits these input data to the host computer/server 16. The host computer/server 16 receives the data and collating the data with the data stored in the data base 18 (Step S9), executes a ticket purchasing step. If a desired ticket cannot be purchased, the host computer/server 16 sends a message stating it to the user terminal device 11 and the step returns to the service menu.

[0025] If a ticket is purchasable, the host computer/server 16 outputs security data from the ticket issue request data and user identification data (Step S10), forms ticket image data from the ticket issue request data (Step S11), and makes ticket printing data by embedding the security data in the ticket image data in the invisible state (Step S12). When the security data is printed on a paper, the security data is visible.

Further, the host computer/server 16 makes ticket display data based on the ticket printing data (Step S13) and transmits the ticket printing data and the ticket display data to the user terminal device 11 (Step S14). The detailed method for making security data, ticket printing data and ticket display data will be described later.

[0026] The ticket display data sent from the host computer/server 16 is displayed on the display of the user terminal device 11 (Step S15). A user checks the display by looking it and when there is no problem, prints a ticket. That is, when a print command is executed, the ticket printing data is sent from the user terminal device 11 to the ticket printer 13 and a ticket 14 is printed and output (Step S16). When the print is normally completed, a print completion command is executed and when there are any print error, etc., the print command is executed again.

[0027] A user is able to go to a place of concert with a printed ticket and use it as usual (Step S17). At the place of concert, whether the used ticket 14 is a proper ticket is checked using a security data detecting system 19. In the security data detecting system 19, the genuineness of the ticket is judged by collating the detected security data with data stored in the data base 18 (Step S18).

[0028] FIG. 3-FIG. 5 show examples of auto race admission tickets applicable to this embodiment. Fig. 3 shows ticket image data 21, FIG. 4 shows security data 22 and FIG. 5 shows ticket printing data schematically.

[0029] The ticket image data 21 shown in FIG. 3 are generated from the ticket issue request data referring to the data base 18 during the process in Step S11 shown in FIG. 2. On this ticket, a kind of ticket 31, a place 32, a data and time 33, a reserved seat number 34, a charge 35, a serial number 36, a ticket issuer 37 and a logo mark that are required for tickets for a normal concert are printed. These data are also printed on the stub of the ticket. The security data 22 shown in FIG. 4 is generated from the user identification data and the ticket issue request data during the process in Step S10 show in FIG. 2. This security data 22 is used for the genuineness judgement to check whether a ticket was forged or altered. In this example, such data as a two-dimensional code data 39, a serial number for inquiring 40, a ticket issuer 41, a logo mark are printed on this ticket. Letters and figures are also expressed in binary image.

[0030] The two-dimensional code data 39 is printed for the automatic mechanical process when the security data 22 is read. The kind of ticket 31, place 32, date and time 33, reserved seat number 34, charge 35, serial number 36, ticket issuer 36 and logo mark 38 were converted into two-dimensional codes and contained in this two-dimensional code data 39. Further, the serial number for inquiry 40, ticket issuer 41 and logo mark are provided for checking the security data 22 with the naked eye.

[0031] Numbers of four figures are used for the inquiry serial numbers 36 and 40 in this embodiment. The tickets shown here are composed of data shown in the following table 1.
<tb><TABLE> Id=[Table 1] Columns=4
<tb>
<tb>Head Col 1: Classification
<tb>Head Col 2: No. of Figure
<tb>Head Col 3: Data Example
<tb>Head Col 4: Use
<tb>Serial No.<SEP>20<SEP>1998092512345678<SEP>Used for inquiry to Data Base
<tb>Date of Issue<SEP>8<SEP>19980925<SEP>Date
<tb>Class. Code 1<SEP>2<SEP>12<SEP>Data Base Class. Code
<tb>Class. Code 2<SEP>4<SEP>3412<SEP>Kind of Ticket/Area/Form of Contract. etc.
<tb>Ticket No.<SEP>6<SEP>345678<SEP>Ticket Issue Order
<tb></TABLE>

[0032] In the above table 1, Date of Issue indicates a date when issue of a ticket was requested, Class. Code 1 indicates the data storage location of the data base for search, Class. Code 2 indicates coded kind of ticket and others, and Ticket No. indicates the ticket issue order. Using a serial number comprising these data as a key for collating to the data base 18, it is possible to uniformly manage a large quantity of tickets.

[0033] Thus, the security data 22 shown in FIG. 4 is able to check both of man and machine. These data are also printed on the stub of a ticket.

[0034] The ticket printing data 23 shown in FIG. 5, that is, visible data and invisible data are made from the security data and the ticket image data during the process of Step S12 shown in FIG. 2 and an actually usable ticket is produced when these data are printed. The ticket printing data 23 shown in FIG. 5 is made by embedding the security data 22 shown in FIG. 4 in the ticket image data 21 shown in FIG. 3 in the invisible state according to a method that is described later. Accordingly, the tickets shown in FIG. 3 and FIG. 5 are quite the same and cannot be discriminated by the naked eye.

[0035] In this embodiment, an inquiry serial number, a ticket issuer and its logo mark are included in the visible state in the ticket image data, and in the invisible state in the security data. Thus, by partially including the data in a ticket in the visible and invisible state, it becomes possible to immediately detect a ticket that is forged or altered through the simple rewriting.

[0036] Further, regarding a logo mark, its location in the visible state is so arranged that it is completely agreed with that in the invisible state. Thus, it becomes very difficult to forge or alter either one or both of logo marks visibly state and invisibly and security of a ticket is further improved.

[0037] Next, how to form the security data will be described.

[0038] The security data is composed of two-dimensional code data and binary image such as letters or marks as shown in FIG. 4; however, one of these elements only or both elements may be included.

[0039] When the security data is input in two-dimensional code, the mechanical process becomes possible when detecting the security data and when the security data is input in binary image, the visual process by man becomes possible and these processes are selectable according to a system characteristic. Two-dimensional code and binary image are called the basic security data.

[0040] One example of the partial generation of the two-dimensional code 39 shown in FIG. 4 will be explained.

[0041] The two-dimensional code 39 is printed on a ticket for the mechanical automatic process when the security data is read as mentioned above, and a kind of ticket, etc. are coded and included on the security data. For two-dimensionally coded data, it is possible to use not only a kind of ticket but also almost all kinds of forms such as voice, image, text, etc. including individual data such as pre-registered voiceprint and fingerprints of user and, managing data.

[0042] First, it is necessary to convert basic security data into digital data. In the case of basic security data comprising such analog data as voice and voiceprint, they are converted into digital data through the A/D conversion. The data that is already in the digital form is used as it is.

[0043] Then, the digitized basic security data is converted into a binary image in two-dimensional code. The basic security data is delimited into 4-bit blocks in order from the top and each block is replaced to a 2x2 pixel black and while binary image according to a value of each block as shown in FIG. 6.

[0044] For instance, when embedded data are arranged in the hexadecimal notation from the top as shown below,
FF 01 45 D3 ...
These data are replaced as shown in FIG. 7.

[0045] Further, the binary image data (FIG. 6) is expanded by n times so as not to impair the embedded image data during the smoothing process at the time of the composite process described later. Here, n=2-4 is desirable. The result when the binary image data shown in FIG. 7 was expanded when, for instance, n=2 is shown in FIG. 8.

[0046] In this embodiment, Calra code was applied in the two-dimensional coding; however, other two-dimensional codes such as matrix system two-dimensional codes and Glyph codes are also usable without problem.

[0047] In the case where such two-dimensional image data as a character string 41 of "Ticket East-West-South-North" and a logo mark 42 as shown in FIG. 4 are inserted in the security data, these data are converted into binary image data. In this case, it is necessary to unify image resolutions when converting data into binary images and is desirable to bring image resolutions in accord with those of the ticket

printing data. Such significant portions including letters, etc. are converted into black components and meaningless portions such as background, etc. are converted into white components.

[0048] The two-dimensional code data and binary image data thus made are arranged in the same size area as the ticket image data as shown in FIG. 4. It is necessary to predetermine the layout by a system for the convenience of a sensor to detect the security data.

[0049] Next, the ticket printing data making method (the composite processing method) will be described in detail.

[0050] The ticket image data 21 is data of a so-called ticket itself and is equivalent to FIG. 3. There are data of 24 bits (8 bits for each of RGB) per pixel. The security data 22 is data to be embedded in the ticket image data 21 in the invisible state and is equivalent to FIG. 4. There are 1 bit data per pixel. The key image data 24 is data that becomes a key for making the ticket printing data and detecting (restoring) the security data. This data is not opened to user and has 1 bit data per pixel.

[0051] First, in the smoothing processing step S51, the smoothing process is executed with the black pixels of the security data made "1" and the white pixels made "0". Here, the pixels at both ends of noteworthy pixels in the x direction are taken, the 3x1 pixel area is cut and a weighted average is taken as shown by the following expression (1).
"(1)" W(i)=(STL(i-1)+2 . STL(i)+STL(i+1))/4
where,

W(i) : x = Weighted mean value of i pixel
STL(i): x = Embedded image data of i pixel = 1 or 0

[0052] If the security data was not increased by n times when made, the two-dimensional code data of the security data was destructed in this smoothing process. The more the expansion factor n is larger, the higher the safe factor not to destruct the embedded image data will become but concealed data is apt to be disclosed.

[0053] For instance, when the key image data 24 and the security data 22 are as shown in FIG. 10 and FIG. 11, respectively, the result of the smoothing process becomes as shown in FIG. 12. The embedded data was expanded to 4 times by setting the security data 22 at n=4. Further, two pixels around the outside are set at "0" as the embedding allowance.

[0054] Then, in the phase modulation step S52, based on the result of the smoothing process in the smoothing process step S51, the phase modulation of the key image data 24 is executed according to the rules of the following expressions (2-1)-(2-3).

"(2-1)" When W(i)=0 -> DES(i)= MSK(i)

"(2-2)" When W(i)=1 -> DES(i)= MSK(i+2)

"(2-3)" When other than above -> DES(i)=MSK(i+1)

DES(i): x=i pixel phase modulation result = 1 or 0
MSK(i): x=i pixel key image data = 1 or 0

[0055] Here, the x=0 column and x=15 column are the edges of the image data and therefore, cannot be smoothed and also cannot be applied with the phase modulation. So, at the edge, the exclusive OR of the key image data 24 with the security data 22 is taken. The result of the phase modulation is shown in FIG. 13.

[0056] Then, in the color difference modulation step S53, based on the phase modulation result in the phase modulation step S52, the color difference modulation process is executed according to the rules of the following expressions (3-1)-(3-6). In this case, three components of R(Red), G(Green) and B(Blue) are

separately calculated. An example of the color difference modulation result of the red component is shown in FIG. 14.

"(3-1)" When DES(i)=1 -> VR(i)= - DELTA V

"(3-2)" -> VG(i)= + DELTA V

"(3-3)" -> VB(i)= + INCREMENT V

"(3-4)" When DES(i)=0 -> VR(i)= + INCREMENT V

"(3-5)" -> VG(i)= - DELTA V

"(3-6)" -> VB(i)= - DELTA V

VR(i): x = the color difference modulation result of i pixel for Red component
An integer in the range of -255 SIMILAR 255
VG(i): x = the color difference modulation result of i pixel for Green component
An integer in the range of -255 SIMILAR 255
VB(i): x = the color difference modulation result of i pixel for Blue component
An integer in the range of -255 SIMILAR 255

[0057] Further, the color difference amount DELTA V is an integer in the range of preset "0 SIMILAR 255". The more the color difference amount DELTA V is larger, the more the visible contract when restoring an embedded image data becomes higher, and the embedded data can be reproduced easily. However, if it is too large, the security data is apt to be easily disclosed. Accordingly, the color difference amount DELTA V is desirable at about "16 SIMILAR 96"; however, DELTA V=48 is used here.

[0058] Lastly, in the superimposition step S54, from the color difference modulation result and the ticket image data 21 in the color difference step S53, the superimposition process shown in the following expression (4-1)-(4-3) is executed and the ticket printing data 23 is made.

"(4-1)" DESR(i)=VR(i)+SRCR(i)

"(4-2)" DESG(i)=VG(i)+SRCG(i)

"(4-3)" DESB(i)=VB(i)+SRCB(i)

DESR(i): x = the i pixel superimposition process result for Red component
An integer in the range of 0 SIMILAR 255.
DESG(i): x = the i pixel superimposition process result for Green component
An integer in the range of 0 SIMILAR 255.
DESB(i): x = the i pixel superimposition process result for Blue Component.
An integer in the range of 0 SIMILAR 255.
SRCR(i): x = Embedded image data of i pixel for Red Component.
An integer in the range of 0 SIMILAR 255.
SRCG(i): x = Embedded image data of i pixel for Green Component.
An integer in the range of 0 SIMILAR 255.
SRCB(i): x = Embedded image data of i pixel for Blue Component.
An integer in the range of 0 SIMILAR 255.

[0059] Further, DESR(i), DESG(i) and DESG(I) are integers in the range of "0 SIMILAR 255", respectively. If the result of calculation is below "0", they are set at "0" and above "255", they are set at "255".

[0060] Results of Red component when all pixels of the ticket image data 21 are (R,G,B)=(127, 127, 127)

are shown in FIG. 15. All values are integers in the range of "0 SIMILAR 255" and "255" indicates that Red component is most frequent. In FIG. 15, pixels with less red components and pixels with much red components are alternately repeated in unit of two pixels in the area where no security data is embedded like a value of (0,0) pixel = 79, a value of (1,0) pixel = 79, a value of (2,0) pixel = 175 ...

[0061] As shown in the expressions (3-1) SIMILAR (3-3) or (3-4) SIMILAR (3-6), red, green and blue color difference amount codes are reversed. Accordingly, in pixels containing much red components, green and blue components are less and in pixels containing less red components, other components are much contained. Red and (Green, Blue) = Cyan are complementary colors each other and even when red and cyan are adjacent to each other, they are hardly discriminated by the eyes of a man and looked as no color. Further, as red rich pixels and cyan rich pixels are arranged repeatedly in unit of several pixels according to key image data, this fine color difference cannot be identified by the eyes of man and a color difference amount is judged to be plus-minus "0".

[0062] For instance, in the expression (4-1), it is erroneously judged to be:
"(5)" DESR(i) SRCR(i)
And it is not possible to discriminated that the image data is embedded. Accordingly, it becomes possible to form a ticket printing data with a security data embedded invisibly in a ticket image data according to this principle.

[0063] When making the print with a color printer using the ticket printing data, the more a color difference amount DELTA V is larger, the more easy to discriminate the data and therefore, the more a degree to restore the security data becomes higher. However, the security data embedded in the invisible state in the ticket printing data may be easily exposed to a third person in some case.

[0064] So, when printing and outputting the ticket printing data with a color printer, it is possible to prevent the security data from being exposed without breaking the security data by outputting the data after executing an error diffusion process as an image processing. The security data in the macroscopically invisible state are preserved because density of pixels of ticket printing data is compensated by the error diffusion process.

[0065] Further, when the error diffusion process is applied, low frequency components decrease and high frequency components increase. As the security data embedded in the ticket printing data is composed of high frequency components, other high frequency components are mixed therein and therefore, the security data becomes the state that is not visually discriminated.

[0066] Next, a ticket display data making method will be described.

[0067] Ticket display data that is made directly unusable is made by partially reducing the ticket printing data and breaking the ticket image data and the security data embedded in the invisible state.

[0068] First, the ticket printing data shown in FIG. 15 is cut in a 3x3 pixel area and is applied with the smoothing process. This is simply to take only an average and the result is as shown in FIG. 16. From the result of the smoothing process, leaving the pixel data at the top of the 4x4 pixel area, the remainder is erased (the thinning process). The result is as shown in FIG. 17. This data becomes the ticket display data.

[0069] Here, amount of data is about 1/4 of the ticket printing data. The print image resolution is generally 300 SIMILAR 600 dpi but the image resolution of the display picture is about 100 dpi, which is 1/3-1/6 of the general print image resolution and therefore, there will be no problem.

[0070] Thus, without displaying the ticket printing data directly on the user terminal device 11, the ticket display data is made by breaking the securing data by reducing data from the ticket printing data and displayed on the user terminal device 11. As the process (display) is fast because amount of data is less and the security data and the ticket image data are partially broken, the ticket printing data cannot be used even when it is tried to obtain it illegally by taking a hard copy of the display. Accordingly, there is such a merit that the security is improved.

[0071] The ticket printing data and the ticket display data are not different apparently from the normal image and therefore, for instance, such general purpose image formats as JPEG (Joint Photographic Experts Group) and TIFF (Tagged Image File Format) are usable. Further, as they can be processed

according to an application for treating general images, the system construction is relatively easy.

[0072] Further, even when the ticket printing data image format is changed to other formats in a system, an embedded security data is left as it is and no problem is caused.

[0073] By the way, the ticket 14 printed with the ticket printing data printed and output with the ticket printer. 13 such as a color printer is used by user at a place of circuit. At this time, the system side is able to judge the genuineness of the ticket by detecting the security data of the used ticket 14. This is described below in detail.

[0074] An image of the ticket 14 printed on a paper, etc. with the ticket printer 13 is read by an optical reading means such as a scanner, digitized to the state shown in FIG. 15 and the security data 22 is restored.

[0075] To restore the security data 22, a key image data 22 shown in FIG. 10 is used. By bringing the key image data 24 to correspond with values of the ticket image of the ticket printing data 23 read by a scanner 1 : 1. The portion "1" of the value of the key image data 24 judges the ticket printing data 23 to be valid and the portion "0" of the value of the key image data 24 judges the value of the ticket printing data 23 to be invalid. The result is shown in FIG. 18. The hatched pixels in the figure are invalid data. The valid data (expressed in white on a black ground) in FIG. 18 is cut out in a prescribed size.

[0076] The security data 22 in this embodiment was expanded by 4 times by setting n=4 and therefore, after removing the embedded allowance of 2 pixels around it, the data is cut out in unit of 4x4 pixels. If a valid data value in he 4x4 pixel range is a red rich value ("175" in this embodiment), the embedded image data (the security data) is 1. If it is a cyan rich value ("79" in this embodiment), the embedded image data is 0. If both of red rich and cyan rich values are included, either one containing more rich color is adopted.

[0077] This is because of the smoothing process in the composition process. The result of the restoration of a embedded image data (the security data) 22 according to this method is shown in FIG. 19. The thick frame portion in the figure is the portion of the security data 22. This portion is in accord with FIG. 11 and it is seen that the security data 22 was completely restored.

[0078] Further, in this embodiment, for instance, after printing the data at a resolution 400 dpi by a thermal sublimation type printer and reading it at a resolution 1200 dpi by an optical scanner, it was restored without any problem.

[0079] Further, as a second security data restoring and detecting method, when a reproduction sheet having the same pattern transmission factor as the key image data 24 is superimposed on the printed surface of the ticket 14 physically, the security data 22 becomes visible. Accordingly, it is possible to directly check a logo mark, etc. in the security data 22 visually. This method does not require troublesome operations and a complicated apparatus and therefore, there is a merit that genuineness of a ticket can be checked simply at any place.

[0080] Further, as a third security data restoring and detecting method, a system to thin a value read by an optical means will be described. It is assume that red components of a value read by a scanner, etc. are as shown in FIG. 15. As a checkered pattern of 4x2 unit is used for the composition process in this embodiment, the security data is thinned in unit of 4 pixels. An expansion factor n when making the security data is also related to this value and an expression of (Checkered grid unit x Expansion factor n $\geq$ Number of pixels to be thinned) becomes valid.

[0081] When the image data shown in FIG. 15 is thinned in unit of 4 pixels, it will become as shown in FIG. 20. However, as image data is insufficient, when all of 4x2 areas are set at the same value with the remaining pixels at the top, the image data becomes as shown in FIG. 21. Although two pixels are deviated in the x direction and the y direction, it is seen that the security data 22 shown in FIG. 11 was completely restored. Thus, when the read image data is thinned, number of pixels to be processed when restoring are reduced and it becomes possible to restore the data at high speed.

[0082] As described above, by detecting the presence of the security data 22 embedded in the used ticket 14, the genuineness of the ticket 14 can be easily judged. For instance, even if the ticket 14 was given to a third person and illegally copied using a color copying machine, the history of that ticket, for instance,

when, where and who issued it can be seen as the security data 22 contains a inquiry serial number and an illegal route can be detected easily.

[0083] In this embodiment, the composition process is executed using a checkered pattern in unit of 4x2 pixels as a key. So, when the composition process is executed using a checkered pattern in size of 1x1 pixel, the effect to prevent the copying with a color copying machine is further promoted. This is because red rich and cyan rich pixel data of the ticket printing data are regularly arranged alternately by the composition process when such square grids as size 1x1 or 2x2 pixels are used.

[0084] A sensor of a scanner portion of a color copying machine is not a spot but has a limited area and therefore, even if a scanner reading resolution is the same as a ticket printing resolution, pixels of a sensor of scanner and pixels of the ticket printing data are finely deviated and they are read as they are. Here, the red and cyan components are complementary colors and it is therefore difficult to separate pixels arranged in extremely highly precise pitches and erroneously recognized to be gray by the eyes of man and sensors, and they cannot be properly copied.

[0085] According to this embodiment, it becomes possible to remarkably promote security of tickets, etc. However, because security data is embedded in the invisible state, some means is needed to restore it and it is not easy to perform this work for all tickets.

[0086] So, it is necessary to distinguish a ticket that has security data embedded in the invisible state from those tickets without security data embedded but guaranteed them to be proper by some other means. For instance, using a means to print a logo mark of a ticket with embedded security data in red and to print a logo mark of a ticket without embedded security in blue, they can be easily checked and time and cost can be saved sharply.

[0087] FIG. 22 schematically shows the state from issue of ticket to detection of security data so far in use. For the ticket image data 21, a landscape photograph is used. For the security data 22, a logo mark "JAPAN" as a copyright data and a two-dimensional code for checking by the sense of vision of a man and by a machine that are converted into the security data according to the steps shown in this embodiment are used.

[0088] First, the ticket printing data 23 is made by executing the composition process of the ticket image data 21, the security data 22 and the key image data 24 according to the method described above. The image of this ticket printing data 23 is seen as a landscape photograph to the eyes of a man but the copyright data, etc. are invisibly embedded. Further, the ticket display data 25 is made from the ticket printing data 23 according to the method shown in this embodiment.

[0089] Then, these ticket printing data 23 and the ticket display data 25 are transmitted via a network to a user who requested the issue of a ticket. When receiving the ticket display data 25, user displays the ticket display data 25 on the display of the user terminal device 11 and after checking its contents, prints and outputs the ticket printing data 23 using the ticket printer 13 as a color printer and obtains the ticket 14.

[0090] User is able to use this issued ticket 14 and a system side detects the security data of the used ticket 14 using the key image data and judges the genuineness of it by collating the data base with the security data.

[0091] As the security data including the copyright data is embedded invisibly in this issued ticket 14, it is possible to restore the copyright data according to the method of restoration described above.

[0092] FIG. 23 is an example of the ticket issue method of this invention applied to an electronic postage stamp. FIG. 23(a) is the ticket printing data, FIG. 23(b) is a stamp image portion and FIG. 23(c) is the security data invisibly embedded in the stamp image portion. To enable a user to issue what has a value equal to money like postage stamps, security becomes particularly important. When security data is invisibly embedded in an electronic postage stamp likewise the auto race admission ticket described above and the print data of that ticket (stamp) is printed directly on an envelope, etc., an electronic stamp can be realized.

[0093] In the case of such a mail, it is generally processed mechanically by an address reader and therefore, security can be maintained by judging its genuineness by reading the security data embedded in an electronic stamp with a sensor. Further, when printing a stamp by a color printer, a cost can be

reduced sharply by simultaneously printing an address and a name.

[0094] As described above, according to this invention, it is possible to provide a ticket issuing method that is capable of easily issuing tickets having high security through such communication means as a network, a telephone line, etc.

[0095] Further, according to this invention, it is possible to provide a ticket collating method that is capable of easily judging the genuineness of issued tickets and easily making a follow-up check when any illegality occurred.

Ticket issuing method, ticket issuing system and ticket collating method

Claims of **EP1014318**

1. A ticket issuing method comprising the steps of:

making security data from ticket issue request data and user identification data sent from a user via a communication means;
making ticket image data from the ticket issue request data;
making ticket printing data by embedding the security data in the ticket image data, the security data being invisible against the ticket image data when the ticket printing data including the ticket image data and the security data is printed on a ticket paper by the user; and
sending the ticket printing data to the user via a communication means.

2. A ticket issuing method according to claim 1, wherein the step to make the security data includes the steps of:

making binary embedded data by binary encoding basic security data comprising control code, letter, image, voice, etc.; and
converting the binary embedded data into binary image data in preset specific format.

3. A ticket issuing method according to claim 1, wherein the step to make the ticket printing data includes the steps of:

making prescribed pattern image data;
making pattern modulated data by modulating the pattern image data by the security data; and
superimposing the pattern modulated image data on the ticket image data.

4. A ticket issuing method according to claim 3, wherein the step of making the prescribed pattern image data includes the step of:

arranging adjacent image data so that they become a combination of complementary colors.

5. A ticket issuing method according to claim 1, further comprising the step of:

making ticket display data for checking the display by a display means of the user by partially reducing the ticket printing data;
wherein the sending step sends the ticket display data together with the ticket printing data to a user via a communication means.

6. A ticket issuing method according to claim 5, wherein the step to make the ticket display data includes the steps of:

executing the smoothing process of the ticket printing data; and
executing the thinning process of the smoothing processed ticket printing data.

7. A ticket issuing method according to claim 1, wherein the ticket printing data making step includes the step of:

embedding a part of the security data in the ticket image data in both the invisible state and the visible state.

8. A ticket issuing method according to claim 1, wherein the ticket printing data making step includes the step of:

embedding a part of the security data in the ticket image data in both the invisible state and the visible state so that the invisible and visible state locations agree with each other.

9. A ticket issuing method according to claim 1, wherein the ticket printing data making step includes the step of:

visibly adding a specific mark for distinguishing from the ticket image data without the security data embedded to the ticket image data with the security data embedded in the invisible state.

10. A ticket issuing method according to claim 1, wherein the security data is composed of user identification data, ticket issue date and time data, kind of ticket data, ticket available period data, ticket charge data and control data.

11. A ticket collating method comprising the steps of:

making security data from ticket issue request data and user identification data sent from a user via a communication means;
making ticket image data from the ticket issue request data;
making a prescribed pattern image data;
making pattern modulated image data by modulating the prescribed pattern image data by the security data;
making ticket printing data by superimposing the pattern modulated image data on the ticket image data;
sending the ticket printing data to the user via a communication means;
restoring the security data from a ticket printed by the user based on the received ticket printing data; and
judging genuineness of the printed ticket according to the restored security data.

12. A ticket collating method according to claim 11, wherein the restoring step includes the step of:

making the security data visible by physically superimposing a sheet shape mask having the transmission factor of the same pattern as the pattern image data on the printed ticket.

13. A ticket collating method according to claim 11, wherein the restoring step includes the step of:

reading the printed ticket data optically and comparing the obtained read signal with a mask signal representing the same pattern as the pattern image data, making the agreed portions of both signals invalid.

14. A ticket collating method according to claim 11, wherein the restoring step includes the step of:

reading the printed ticket data optically and executing the thinning process of the obtained read signal at the period corresponding to spacial frequency of the pattern image data.

15. A ticket issuing system comprising:

means for making security data from ticket issue request data and user identification data sent from a user via a communication means;
means for making ticket image data from the ticket issue request data;
means for making ticket printing data by embedding the security data in the ticket image data, the security data being invisible against the ticket image data when the ticket printing data including the ticket image data and the security data is printed on a ticket paper by the user; and
means for sending the ticket printing data to the user via the communication means.

16. A ticket issuing method comprising the steps of:

outputting security data according to ticket issue request data from a user via a communication means, the security data being visible when the security data is printed on a paper;
outputting ticket image data from the ticket issue request data, the ticket image data being visible when the ticket image data is printed on a paper;
outputting ticket printing data by embedding the security data in the ticket image data, the security data being invisible against the ticket image data when the ticket printing data including the ticket image data and the security data is printed on a ticket paper by the user; and
sending the ticket printing data to the user via the communication means.

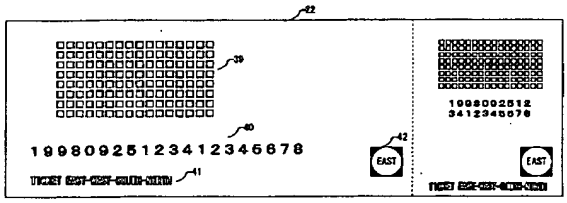

FIG. 4

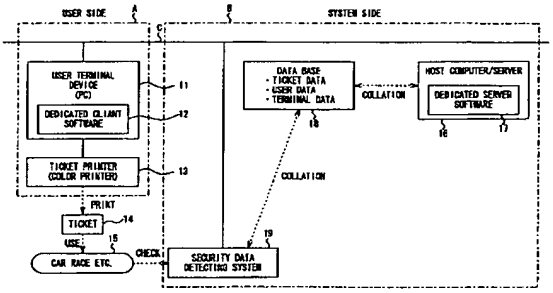

FIG. 1

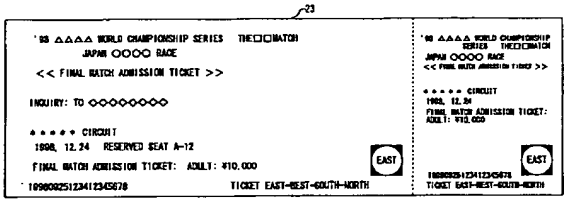

FIG. 5

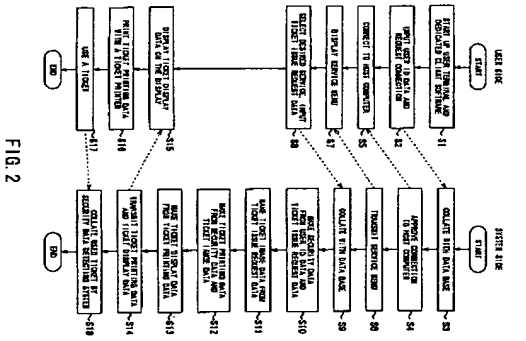

FIG. 2

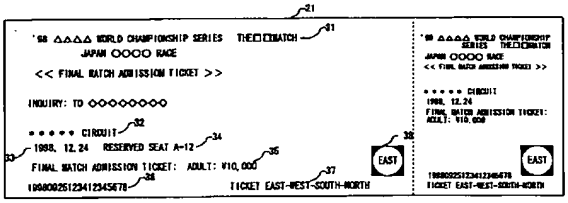

FIG. 3

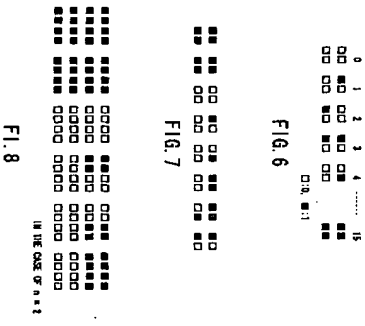

FIG. 6

FIG. 7

FIG. 8